УДК 519.7

О ШИФРАХ, НЕ РАСПРОСТРАНЯЮЩИХ ИСКАЖЕНИЙ
ON CIPHERS, NOT SPREADING DISTORTIONS

Рацеев С.М., Рацеев В.М.
Ratseev S.M., Ratseev V.M.

Ульяновский государственный университет, 432017, г. Ульяновск, ул. Льва Толстого, 42.
Ulyanovsk State University, 432017, Ulyanovsk, Lev Tolstoy 42
E-mail: ratseevsm@mail.ru

E-mail: galtsev_o@.bsu.edu.ru; galtseva@ bsu.edu.ru

Ключевые слова: шифр, модель шифра, искажение сообщения.
Key words: cipher, cipher model, distortion of the message.

Аннотация. В работе приводится систематическое изложение материала по описанию эндоморфных шифров, не распространяющих искажений. Данная работа основана на работах [1] и [2].
Resume. The paper provides systematic presentation of the material according to the description of the ciphers, not distributing distortions. This work is based on the works [1] and [2].

Введение

Следуя работе [1], введем алгебраическую модель шифра. Пусть X, K, Y — некоторые (не обязательно конечные) множества возможных открытых текстов, ключей и шифрованных текстов соответственно. Пусть также $E_k : X \to Y$ — правило зашифрования на ключе $k \in K$. Обозначим через E множество правил зашифрования $\{E_k \mid k \in K\}$, а через $E_k(X)$ — образ множества X при отображении $E_k : X \to Y$, т.е. $E_k(X) = \{E_k(x) \mid x \in X\}$. Пусть $D_k : E_k(X) \to X$ — правило расшифрования на ключе $k \in K$. Обозначим через D множество правил расшифрования $\{D_k \mid k \in K\}$.

Определение 1. *Шифром (шифросистемой) называется совокупность*

$$\Sigma_A = (X, K, Y, E, D),$$

для которой выполнены следующие свойства:

1) для любых $x \in X$ и $k \in K$ выполнено равенство $D_k(E_k(x)) = x$;

2) $Y = \bigcup_{k \in K} E_k(X)$.

В обзорной работе [3] рассматриваются задачи построения совершенных шифров по заданному набору параметров, приводятся необходимые и достаточные условия данных шифров, рассматриваются совершенные шифры замены с неограниченным ключом, а также совершенные шифры, стойкие к имитации и подмене шифрованных сообщений с необязательно равномерным распределением на множестве ключей.

Передаваемое по каналу связи шифрованное сообщение может подвергнуться как целенаправленным искажениям злоумышленников, так и искажениям, причиной которых могут являться помехи в самом канале связи. Искажения могут привести к потере части или даже всего открытого текста, так как расшифрование искаженного шифрованного текста может привести к непредсказуемым результатам. Нас будут интересовать шифры, которые не распространяют искажения при расшифровании. Ограничимся рассмотрением эндоморфных шифров и таких

искажений, которые заменяют символы алфавита символами того же алфавита, либо приводят к потере или появлению дополнительных символов алфавита.

Пусть A — некоторый конечный алфавит. На протяжении всей работы считается, что $X = Y = \bigcup_{l=1}^{\infty} A^l$.

Шифры, не распространяющие искажений типа замены знаков

Рассмотрим шифры, которые не изменяют длины сообщения при шифровании, т.е. такие шифры $\Sigma_A = (X, K, Y, E, D)$, что для любого $l \in \mathbb{N}$, любого $x \in A^l$ и любого $k \in K$ следует, что $E_k(x) \in A^l$. Поэтому $E_k(A^l) \subseteq A^l$ для любого $l \in \mathbb{N}$ и $k \in K$.

Так как все правила зашифрования E_k являются инъективными отображениями множества X в Y, то, с учетом того, что $X = Y$, все E_k будут являться также биективными преобразованиями множества X. В частности, $E_k(A^l) = A^l$ для любого $l \in \mathbb{N}$ и $k \in K$.

В A^l для любого $l \in \mathbb{N}$ введем метрику Хэмминга, определенную следующей формулой:

$$\rho(x, y) = \sum_{i=1}^{l} \delta(x_i, y_i),$$

где $x = x_1 \dots x_l$, $y = y_1 \dots y_l \in A^l$, причем

$$\delta(x_i, y_i) = \begin{cases} 1, & x_i \neq y_i, \\ 0, & x_i = y_i. \end{cases}$$

Пусть $r > 0$ и $x \in A^l$. Определим шар радиуса r с центром в x как множество

$$S_r(x) = \{y \in A^l \mid \rho(x, y) \leq r\}.$$

Определение 2. *Говорят, что шифр Σ_A не распространяет искажений типа замены знаков, если для любого $l \in \mathbb{N}$, любых $x, y \in A^l$ и $k \in K$ выполнено неравенство*

$$\rho(D_k(x), D_k(y)) \leq \rho(x, y).$$

Лемма 1. *Для эндоморфного шифра Σ_A, не изменяющего длины сообщений, следующие условия эквивалентны.*

(i) Шифр Σ_A не распространяет искажений типа замены знаков.

(ii) Для любого $l \in \mathbb{N}$, любых $x, y \in A^l$ и $k \in K$ выполнено равенство

$$\rho(D_k(x), D_k(y)) = \rho(x, y). \tag{1}$$

(iii) Для любого $l \in \mathbb{N}$, любых $x, y \in A^l$ и $k \in K$ выполнено равенство

$$\rho(E_k(x), E_k(y)) = \rho(x, y).$$

Доказательство. Очевидно, что если выполняется равенство (1), то шифр Σ_A не распространяет искажений типа замены знаков, поэтому из (ii) следует (i).

Докажем в обратную сторону. Зафиксируем некоторое $l \in \mathbb{N}$ и некоторый элемент $k \in K$. Рассмотрим следующее преобразование f множества $A^l \times A^l$:

$$f(x, y) = (D_k(x), D_k(y)), \ (x, y) \in A^l \times A^l.$$

Так как D_k является биективным преобразованием множества A^l, то преобразование f множества $A^l \times A^l$ также является биективным. Поэтому если (x, y) пробегает все множество $A^l \times A^l$, то $(D_k(x), D_k(y))$ также пробегает все множество $A^l \times A^l$. Следовательно,

$$\sum_{(x,y)\in A^l\times A^l} \rho(D_k(x), D_k(y)) = \sum_{(x,y)\in A^l\times A^l} \rho(x, y).$$

Из данного равенства следует, что

$$\sum_{(x,y)\in A^l\times A^l} [\rho(x, y) - \rho(D_k(x), D_k(y))] = 0.$$

Так как все слагаемые последней суммы неотрицательны и вся сумма равна 0, то это возможно лишь в том случае, когда выполнено условие (1). Следовательно, условие (i) влечет условие (ii).

Пусть выполнено условие (ii). Тогда

$$\rho(E_k(x), E_k(y)) = \rho(D_k(E_k(x)), D_k(E_k(y))) = \rho(x, y).$$

Таким образом, из (ii) следует (iii).

Обратно, пусть выполнено условие (iii). Тогда

$$\rho(D_k(x), D_k(y)) = \rho(E_k(D_k(x)), E_k(D_k(y))) = \rho(x, y).$$

Поэтому условие (iii) влечет условие (ii). Лемма доказана.

Отображение $f : A^l \to A^l$ называется *изометрией*, если для любых $x, y \in A^l$ выполнено равенство

$$\rho(f(x), f(y)) = \rho(x, y).$$

Заметим, что из определения изометрии следует, что f является биективным преобразованием множества A^l.

Лемма 1 показывает, что если эндоморфный шифр Σ_A не распространяет искажений типа замены знаков, то множество правил зашифрования E состоит из изометрий.

Зафиксируем произвольным образом элемент $\bar{a} = a_1 \ldots a_l \in A^l$. Обозначим

$$S_1^i(\bar{a}) = \{a_1 \ldots a_{i-1} a a_{i+1} \ldots a_l \mid a \in A\}.$$

Заметим, что

$$\bigcup_{i=1}^{l} S_1^i(\bar{a}) = S_1(\bar{a}), \quad \bigcap_{i=1}^{l} S_1^i(\bar{a}) = \begin{cases} A, & l = 1, \\ \{\bar{a}\}, & l > 1. \end{cases} \tag{2}$$

Лемма 2. *Пусть $f : A^l \to A^l$ — изометрия и $\bar{a} = a_1 \ldots a_l$ — некоторый элемент из A^l. Тогда будут выполнены следующие условия.*

1. Для любого $r \geq 1$ справедливо равенство

$$f(S_r(\bar{a})) = S_r(f(\bar{a})). \tag{3}$$

2. Для любого $i = 1,2,\ldots,l$ найдется такое j, $1 \leq j \leq l$, зависящее от значения i, что будет выполнено равенство

$$f(S_1^i(\bar{a})) = S_1^j(f(\bar{a})). \tag{4}$$

Доказательство. 1. Пусть $r \geq 1$ — некоторое число. Покажем, что выполнено включение $f(S_r(\bar{a})) \subseteq S_r(f(\bar{a}))$. Пусть $\bar{y} \in f(S_r(\bar{a}))$. Тогда найдется такой элемент $\bar{x} \in S_r(\bar{a})$, что $f(\bar{x}) = \bar{y}$. При этом

$$\rho(f(\bar{a}), \bar{y}) = \rho(f(\bar{a}), f(\bar{x})) = \rho(\bar{a}, \bar{x}) \leq r.$$

Следовательно, $\bar{y} \in S_r(f(\bar{a}))$, что показывает включение $f(S_r(\bar{a})) \subseteq S_r(f(\bar{a}))$. Поскольку

$$|S_r(\bar{a})| = |f(S_r(\bar{a}))| = |S_r(f(\bar{a}))|,$$

то выполнено равенство (3).

2. Чтобы доказать равенство (4), достаточно показать, что выполнено вложение

$$f(S_1^i(\bar{a})) \subseteq S_1^j(f(\bar{a})),$$

так как $|f(S_1^i(\bar{a}))| = |S_1^j(f(\bar{a}))|$ для любых $1 \leq i, j \leq l$.

Предположим противное. Пусть существует такое i_0, что для любого $j = 1,2,\ldots,l$

$f(S_1^{i_0}(\bar{a}))$ не содержится в $S_1^j(f(\bar{a}))$.

Заметим, что из (2) и пункта 1 данной леммы следует, что

$$f\left(\bigcup_{i=1}^{l} S_1^i(\bar{a})\right) = \bigcup_{j=1}^{l} S_1^j(f(\bar{a})).$$

Поэтому найдутся такие $\bar{x}_1, \bar{x}_2 \in S_1^{i_0}(\bar{a})$, причем $\bar{x}_1 \neq \bar{a}$ и $\bar{x}_2 \neq \bar{a}$, и такие $j_1 < j_2$, что $\bar{y}_1 = f(\bar{x}_1) \in S_1^{j_1}(f(\bar{a}))$ и $\bar{y}_2 = f(\bar{x}_2) \in S_1^{j_2}(f(\bar{a}))$.

Пусть $f(\bar{a}) = c_1 \ldots c_l$. Тогда

$$\bar{y}_1 = c_1 \ldots c_{j_1-1} d c_{j_1+1} \ldots c_{j_2-1} c_{j_2} c_{j_2+1} \ldots c_l,$$

$$\bar{y}_2 = c_1 \ldots c_{j_1-1} c_{j_1} c_{j_1+1} \ldots c_{j_2-1} e c_{j_2+1} \ldots c_l,$$

причем $d \neq c_{j_1}$ и $e \neq c_{j_2}$. Поэтому $\rho(\bar{y}_1, \bar{y}_2) = 2$. Но

$$\rho(\bar{y}_1, \bar{y}_2) = \rho(f(\bar{x}_1), f(\bar{x}_2)) = \rho(\bar{x}_1, \bar{x}_2) = 1.$$

Противоречие. Лемма доказана.

Лемма 3. *Пусть* $f, g : A^l \to A^l$ *— изометрии. Тогда*

(i) если для некоторого $\bar{a} \in A^l$ выполнено равенство $f|_{S_1(\bar{a})} = id|_{S_1(\bar{a})}$, где id — тождественное отображение, то $f = id$ на всем множестве A^l;

(ii) если для некоторого $\bar{a} \in A^l$ выполнено равенство $f|_{S_1(\bar{a})} = g|_{S_1(\bar{a})}$, то $f = g$ на всем множестве A^l. **Доказательство.** (i) Рассмотрим последовательность шаров:

$$S_1(\bar{a}) \subseteq S_2(\bar{a}) \subseteq \ldots \subseteq S_n(\bar{a}) \subseteq \ldots$$

Заметим, что данная последовательность является стабилизирующейся, так как для любого $n \geq l$ выполняется равенство $S_n(\bar{a}) = A^l$. С помощью индукции покажем, что для любого $n \geq 1$ сужение отображения f на множество $S_n(\bar{a})$ равно тождественной функции на множестве $S_n(\bar{a})$:

$$f|_{S_n(\bar{a})} = id|_{S_n(\bar{a})},$$

Из условия (i) леммы база индукции при $n=1$ выполняется.

Предположим, что сужение отображения f на множество $S_k(\bar{a})$ для любого $k<n$ является тождественным отображением. Покажем, что $f|_{S_n(\bar{a})} = id|_{S_n(\bar{a})}$, т.е. для любого $\bar{b} \in S_n(\bar{a})$ выполнено равенство $f(\bar{b}) = \bar{b}$. Не ограничивая общность, рассмотрим в качестве $\bar{b}$ такой элемент:

$$\bar{b} = b_1 b_2 \ldots b_n a_{n+1} \ldots a_l.$$

Если $\rho(\bar{a},\bar{b}) < n$, тогда по предположению индукции выполнено равенство $f(\bar{b}) = \bar{b}$. Поэтому рассмотрим случай $\rho(\bar{a},\bar{b}) = n$, который означает, что $a_1 \neq b_1$, $a_2 \neq b_2$,... , $a_n \neq b_n$. Введем в рассмотрение следующие элементы шара $S_{n-1}(\bar{a})$:

$$\bar{b}_1 = a_1 b_2 \ldots b_n a_{n+1} \ldots a_l,$$

$$\bar{b}_2 = b_1 a_2 \ldots b_n a_{n+1} \ldots a_l,$$

$$\bar{b}_n = b_1 b_2 \ldots a_n a_{n+1} \ldots a_l.$$

По предположению индукции $f(\bar{b}_i) = \bar{b}_i$ для любого $i = 1,2,\ldots,n$. Поэтому

$$\rho(f(\bar{b}),\bar{b}_i) = \rho(f(\bar{b}), f(\bar{b}_i)) = \rho(\bar{b},\bar{b}_i) = 1.$$

Следовательно,

$$f(\bar{b}) \in \bigcap_{i=1}^{n} S_1(\bar{b}_i).$$

При этом

$$\bigcap_{i=1}^{n} S_1(\bar{b}_i) = \begin{cases} \{\bar{a},\bar{b}\}, & n = 2, \\ \{\bar{b}\}, & n > 2. \end{cases}$$

Так как f является биективным преобразованием множества A^l и $f(\bar{a}) = \bar{a}$, то $f(\bar{b}) = \bar{b}$.

(ii) Пусть для некоторого $\bar{a} \in A^l$ выполнено равенство $f|_{S_1(\bar{a})} = g|_{S_1(\bar{a})}$.

Так как f и g биективные преобразования множества A^l, являющиеся изометриями, то преобразование $f \circ g^{-1}$ также будет являться биективным преобразованием множества A^l и изометрией, причем

$$(f \circ g^{-1})|_{S_1(\bar{a})} = id|_{S_1(\bar{a})}.$$

Поэтому из пункта (i) будет следовать, что

$$f \circ g^{-1} = id$$

на всем множестве A^l. Следовательно, $f = g$ на множестве A^l. Лемма доказана.

Пусть $l \in \mathbb{N}$. Определим на множестве A^l такие преобразования:

$$\Pi_{j_1 \ldots j_l}(a_1 \ldots a_l) = a_{j_1} \ldots a_{j_l},$$

$$R(a_1 \ldots a_l) = R_1(a_1) \ldots R_l(a_l),$$

где $R_1,\dots,R_l$ — некоторые подстановки множества A, $\Pi_{j_1\dots j_l}$ — некоторая перестановка:

$$\Pi_{j_1\dots j_l}=\begin{pmatrix}1 & 2 & \dots & l\\ j_1 & j_2 & \dots & j_l\end{pmatrix}$$

Теорема 1 (Марков А.А.). *Отображение $E_k\in E$ является изометрией тогда и только тогда, когда для любого $l\in\mathbb{N}$*

$$E_k|_{A^l}=R\circ\Pi_{j_1\dots j_l}$$

для подходящих R и $\Pi_{j_1\dots j_l}$, где $E_k|_{A^l}$ — сужение отображения E_k на множество A^l.

Доказательство. Так как преобразования R и $\Pi_{j_1\dots j_l}$ являются изометриями, а композиция изометрий также является изометрией, то достаточность условия теоремы очевидна.

Докажем в обратную сторону. Зафиксируем произвольное значение $l\in\mathbb{N}$ и некоторый элемент $\bar{a}=a_1\dots a_l\in A^l$. Пусть $E_k(a_1\dots a_l)=c_1\dots c_l$. Из второго пункта леммы 2 следует, что для любого $i=1,2,\dots,l$ найдется такое $j=j(i)$, что

$$E_k:\{a_1\dots a_{i-1}aa_{i+1}\dots a_l\mid a\in A\}\to\{c_1\dots c_{j-1}ac_{j+1}\dots c_l\mid a\in A\}.$$

Поэтому

$$E_k(a_1\dots a_{i-1}aa_{i+1}\dots a_l)=c_1\dots c_{j-1}R_{j_i}(a)c_{j+1}\dots c_l, \tag{5}$$

где R_{j_i} — некоторая подстановка множества A. Следовательно, сужение отображения E_k на множество $S_1(\bar{a})$ представимо в виде композиции преобразований R и $\Pi_{j_1\dots j_l}$:

$$E_k|_{S_1(\bar{a})}=(R\circ\Pi_{j_1\dots j_l})|_{S_1(\bar{a})},$$

где $R_1,\dots,R_l$ — преобразования, полученные в формуле (5). Так как композиция изометрий R и $\Pi_{j_1\dots j_l}$ также является изометрией, то из последнего равенства в силу леммы 3 следует такое равенство:

$$E_k|_{A^l}=R\circ\Pi_{j_1\dots j_l}.$$

Теорема доказана.

Из теоремы А.А. Маркова следует, что в классе эндоморфных шифров, не изменяющих длины сообщений, не распространяют искажений типа замены знаков, например, шифры перестановки, поточные шифры однозначной замены, а так же композиции шифров перестановки и замены.

Шифры, не распространяющие искажений типа пропуска знаков

Данный параграф написан на основе работы [2]. Здесь рассматриваются эндоморфные шифры и такие искажения, которые приводят к потере символов алфавита.

Введем на множестве $X=Y$ бинарное отношение ε следующим образом. Пусть $x,y\in X$. $x\varepsilon y \Leftrightarrow$ слово y получено из x путем удаления одного вхождения некоторой его буквы. Определим множество $\varepsilon(x)$ для некоторого $x\in X$ следующим образом:

$$\varepsilon(x)=\{y\in X \mid x\varepsilon y\}.$$

Например, если $x=x_1x_2x_3$, то $\varepsilon(x)=\{x_1x_2, x_1x_3, x_2x_3\}$.

Через ε^n будем понимать степень отношения ε: $x\varepsilon^n y$, где значение n меньше длины слова x, тогда и только тогда, когда слово y получено из x путем удаления n вхождений некоторых его букв. Можно также дать и эквивалентное определение для ε^n: $x\varepsilon^n y$, где значение n меньше длины слова x, тогда и только тогда, когда найдутся такие z_1, z_2,..., $z_{n-1}\in X$, что

$$x\,\varepsilon\, z_1\,\varepsilon\, z_2\,\varepsilon\ldots\varepsilon\, z_{n-1}\,\varepsilon\, y.$$

Заметим, что $x\varepsilon^0 y \Leftrightarrow x=y$.

Определение 3. *Будем говорить, что шифр Σ_A не распространяет искажений типа пропуска знаков, если для любых $x,y\in Y$, любого $k\in K$ и любого натурального n, меньшего длины слова x, найдется такое число $0\le m\le n$, что из условия $x\varepsilon^n y$ следует $D_k(x)\varepsilon^m D_k(y)$.*

Лемма 4. *Если в определении 3 число $n>0$, то из этого всегда будет следовать, что число m также больше нуля.*

Доказательство. Пусть для некоторых $x,y\in Y$ из условия $x\varepsilon^n y$ следует $D_k(x)\varepsilon^0 D_k(y)$, где n — некоторое положительное число, меньшее длины слова x, и k — некоторый элемент множества K. Так как $x\varepsilon^n y$, то $x\neq y$, а из условия $D_k(x)\varepsilon^0 D_k(y)$ следует, что $D_k(x)=D_k(y)$, что противоречит инъективности отображения D_k. Лемма доказана.

Лемма 5. *Если эндоморфный шифр Σ_A не распространяет искажений типа пропуска знаков, то он не изменяет длины сообщений при шифровании.*

Доказательство. Пусть выполнено условие леммы для некоторого шифра Σ_A. Покажем, что для любого $k\in K$ и любого $l\in\mathbb{N}$ выполнено включение $E_k(A^l)\subseteq A^l$.

Фиксируем произвольное $k\in K$. Рассмотрим сначала случай $l=1$. Предположим, что $E_k(A)$ не содержится в A, то есть найдется такое $a\in A$, что $E_k(a)=b_1\ldots b_t\in A^t$, где $t>1$. Так как $b_1\ldots b_t\varepsilon b_1\ldots b_{t-1}$, то $D_k(b_1\ldots b_t)\varepsilon D_k(b_1\ldots b_{t-1})$. Но $D_k(b_1\ldots b_t)=a\in A$, а длина слова $D_k(b_1\ldots b_{t-1})$ не меньше единицы, поэтому, с учетом леммы 4, пришли к противоречию. Следовательно, $E_k(A)\subseteq A$.

Предположим, что для всех $t<l$, где $l>1$, выполнено включение $E_k(A^t)\subseteq A^t$ для любого $k\in K$. Покажем, что тогда $E_k(A^l)\subseteq A^l$. Предположим, что это не так для некоторого $k\in K$. Пусть $E_k(A^l)$ не содержится в A^l, т.е. найдется такое $x\in A^l$, что $E_k(x)=b_1\ldots b_s$, причем $s\neq l$. Заметим, что число s не может быть меньше чем l, так как $D_k(A^t)\subseteq A^t$ для всех $t<l$. Поэтому $s>l$. Из отношения $b_1\ldots b_s\varepsilon b_1\ldots b_{s-1}$ должно следовать отношение $D_k(b_1\ldots b_s)\varepsilon D_k(b_1\ldots b_{s-1})$, но длина слова $D_k(b_1\ldots b_s)$ равна l, а длина слова $D_k(b_1\ldots b_{s-1})$ не меньше l, что следует из предположения индукции, так как $s-1\geq l$. Поэтому пришли к противоречию. Следовательно $E_k(A^l)\subseteq A^l$. Лемма доказана.

Лемма 6. *Для эндоморфного шифра Σ_A следующие условия эквивалентны.*

(i) Шифр Σ_A не распространяет искажений типа пропуска знаков.

(ii) Для любых $x,y\in Y$, любого $k\in K$ и любого натурального n, меньшего длины слова x, из условия $x\varepsilon^n y$ следует $D_k(x)\varepsilon^n D_k(y)$.

(iii) Для любых $x,y\in X$, любого $k\in K$ и любого натурального n, меньшего длины слова x, из условия $x\varepsilon^n y$ следует $E_k(x)\varepsilon^n E_k(y)$.

Доказательство. Очевидно, что из условия (ii) следует (i).

Докажем в обратную сторону. Предположим, что выполнено условие (i). Пусть $x,y\in Y$ и $x\varepsilon^n y$, т.е. найдутся такие z_1, z_2 ,..., $z_{n-1}\in Y$, что

$$x\,\varepsilon\, z_1\,\varepsilon\, z_2\,\varepsilon\ldots\varepsilon\, z_{n-1}\,\varepsilon\, y.$$

Тогда, учитывая лемму 4, имеем

$$D_k(x)\,\varepsilon\, D_k(z_1)\,\varepsilon\, D_k(z_2)\,\varepsilon\ldots\varepsilon\, D_k(z_{n-1})\,\varepsilon\, D_k(y).$$

Следовательно, $D_k(x)\varepsilon^n D_k(y)$. Поэтому условие (i) влечет условие (ii).

Пусть выполнено условие (ii). Зафиксируем некоторое значение $k\in K$. Пусть $x,y\in X$. Так как шифр Σ_A сохраняет длины сообщений при шифровании (лемма 5), то найдется такое число m, что

$$D_k^m(x)=\underbrace{(D_k\circ\ldots\circ D_k)}_{m}(x)=x,\quad D_k^m(y)=\underbrace{(D_k\circ\ldots\circ D_k)}_{m}(y)=y.$$

Поэтому $E_k(x)=D_k^{m-1}(x)$ и $E_k(y)=D_k^{m-1}(y)$. Так как из отношения $x\varepsilon^n y$ следует $D_k(x)\varepsilon^n D_k(y)$, из которого, в свою очередь, следует $D_k^2(x)\varepsilon^n D_k^2(y)$ и т.д., то

$$E_k(x)=D_k^{m-1}(x)\,\varepsilon^n\, D_k^{m-1}(y)=E_k(y).$$

Таким образом, из условия (ii) следует (iii).

Аналогичным образом доказывается, что условие (iii) влечет условие (ii). Лемма доказана.

Лемма 7. *Пусть эндоморфный шифр Σ_A не распространяет искажений типа пропуска знаков. Тогда для любого $x\in X$ и любого $k\in K$ следует равенство*

$$E_k(\varepsilon(x))=\varepsilon(E_k(x)).$$

Доказательство. Зафиксируем $x \in X$ и $k \in K$. Покажем сначала, что

$$E_k(\varepsilon(x)) \subseteq \varepsilon(E_k(x)). \tag{6}$$

Пусть $y \in E_k(\varepsilon(x))$. Тогда найдется такой $x' \in \varepsilon(x)$, что $y = E_k(x')$. Так как $x \varepsilon x'$, то $E_k(x) \varepsilon E_k(x') = y$ (лемма 6). Следовательно, $y \in \varepsilon(E_k(x))$, что доказывает включение (6).

Аналогичным же образом получается, что

$$D_k(\varepsilon(x)) \subseteq \varepsilon(D_k(x)),$$

из которого следует, что

$$D_k(\varepsilon(E_k(x))) \subseteq \varepsilon(D_k(E_k(x))) = \varepsilon(x). \tag{7}$$

Из включения (7) следует такое включение:

$$\varepsilon(E_k(x)) = E_k(D_k(\varepsilon(E_k(x)))) \subseteq E_k(\varepsilon(x)).$$

Лемма доказана.

Лемма 8. *Пусть $\bar{x}, \bar{y} \in A^l$ для некоторого $l \geq 3$. Тогда из равенства $\varepsilon(\bar{x}) = \varepsilon(\bar{y})$ будет следовать равенство $\bar{x} = \bar{y}$.*

Доказательство. Докажем сначала, что любое слово $\bar{x} \in A^l$, где $l \geq 3$, однозначно определяется множеством $\varepsilon(\bar{x})$.

Пусть a — первый символ слова $\bar{x}$. Тогда возможны 3 случая:

1) $\bar{x} = a^l = \underbrace{a \ldots a}_{l},$
2) $\bar{x} = a^n b\bar{z}, \quad n \geq 2, b \in A, a \neq b,$
3) $\bar{x} = ab\bar{z}, \quad b \in A, a \neq b.$

В первом случае множество $\varepsilon(\bar{x})$ состоит из одного слова a^{l-1}.

Во втором случае все слова из $\varepsilon(\bar{x})$ начинаются с буквы a, причем одно из них есть $a^{n-1}b\bar{z}$, а все другие имеют начало a^n.

В третьем случае $\varepsilon(\bar{x})$ содержит слова $a\bar{z}$ и $b\bar{z}$, а все остальные слова (если они есть, т.е. $\bar{z} \neq b^{l-2}$) имеют начало ab.

Поэтому алгоритм восстановления слова $\bar{x}$ по множеству $\varepsilon(\bar{x})$ будет следующим.

1. Если $\varepsilon(\bar{x}) = \{a^{l-1}\}$, то $\bar{x} = a^l$.

2. Если все слова из $\varepsilon(\bar{x})$ начинаются на одну и ту же букву, например, a, то одним из них является $a^{n-1}b\bar{z}$, а все остальные имеют вид $a^n z_i$. Тогда $\bar{x} = a^n b\bar{z}$.

3. Пусть все слова, кроме одного, множества $\varepsilon(\bar{x})$ начинаются на одну и ту же букву.

a) Если $\varepsilon(\bar{x}) = \{a\bar{z}, b\bar{z}\}$, то либо $\bar{z} = a^{l-2}$, либо $\bar{z} = b^{l-2}$. Поэтому если, например, $\bar{z} = b^{l-2}$, то $\bar{x} = ab^{l-1}$.

b) Если же $\varepsilon(\bar{x}) = \{a\bar{z}, b\bar{z}, ab\bar{z}_1, \ldots, ab\bar{z}_m\}$, то из множества $\varepsilon(\bar{x})$ возьмем единственное слово, не начинающееся на букву a, то есть $b\bar{z}$, и добавим к нему в начало букву a, получаем $\bar{x} = ab\bar{z}$.

Таким образом, если $\varepsilon(\overline{x}) = \varepsilon(\overline{y})$ для некоторых $\overline{x}, \overline{y} \in A^l$, где $l \geq 3$, то $\overline{x} = \overline{y}$. Лемма доказана.

Обозначим через σ такое биективное преобразование множества X, для которого выполнено свойство $\sigma(x_1 \ldots x_l) = \sigma(x_1) \ldots \sigma(x_l)$ для любого $x = x_1 \ldots x_l \in X$. Таким образом, преобразование σ достаточно задать на множестве A. Обозначим также через μ оператор обращения слов, т.е. если $x = x_1 \ldots x_l$, то $\mu(x) = x_l \ldots x_1$.

Теорема 2 (Бабаш А.В., Глухов М.М., Шанкин Г.П.**).** *Пусть* $X = Y = \bigcup_{l=1}^{L} A^l$. *Эндоморфный шифр* Σ_A *не распространяет искажений типа пропуска знаков тогда и только тогда, когда для любого* $k \in K$ *выполнены следующие условия:*

1. Если $L = 2$, то для любого $x \in X$ либо

$$E_k(x) = \sigma(x),$$

либо

$$E_k(x) = \sigma(\mu(x)),$$

где $\sigma = E_k|_A$ — сужение отображения E_k на множество A;

2. Если $L > 2$, то либо

$$E_k = \sigma \text{ на всем множестве } X,$$

либо

$$E_k = \sigma \circ \mu \text{ на всем множестве } X,$$

где $\sigma = E_k|_A$ — сужение отображения E_k на множество A.

Доказательство. Очевидно, что отображения σ и μ не распространяют искажений типа пропуска знаков, поэтому достаточность условия теоремы очевидна.

Докажем в обратную сторону. Зафиксируем $k \in K$.

1. Пусть $L = 2$. Так как шифр Σ_A не изменяет длины слов при шифровании (лемма 5), то $E_k(A) = A$. Обозначим через σ — сужение отображения E_k на множество A. Покажем, что для любого $a_1 a_2 \in A^2$ либо $E_k(a_1 a_2) = \sigma(a_1)\sigma(a_2)$, либо $E_k(a_1 a_2) = \sigma(a_2)\sigma(a_1)$.

Пусть $a_1 \neq a_2$ и $E_k(a_1 a_2) = b_1 b_2 \in A^2$. Из леммы 7 следует, что

$$E_k(\varepsilon(a_1 a_2)) = \varepsilon(E_k(a_1 a_2)).$$

Так как

$$E_k(\varepsilon(a_1 a_2)) = E_k(\{a_1, a_2\}) = \{E_k(a_1), E_k(a_2)\} = \{\sigma(a_1), \sigma(a_2)\},$$

$$\varepsilon(E_k(a_1 a_2)) = \varepsilon(b_1 b_2) = \{b_1, b_2\},$$

то либо $\sigma(a_1) = b_1$ и $\sigma(a_2) = b_2$, либо $\sigma(a_1) = b_2$ и $\sigma(a_2) = b_1$.

Пусть $a_1 = a_2 = a$ и $E_k(aa) = b_1 b_2$. Тогда

$$E_k(\varepsilon(aa)) = E_k(\{a\}) = \{\sigma(a)\},$$

$$\varepsilon(E_k(aa)) = \varepsilon(b_1 b_2) = \{b_1, b_2\}.$$

Следовательно, $b_1 = b_2 = \sigma(a)$.

2. Пусть $L > 2$. Из пункта 1 следует, что для любого $a_1a_2 \in A^2$ либо $E_k(a_1a_2) = \sigma(a_1)\sigma(a_2)$, либо $E_k(a_1a_2) = \sigma(a_2)\sigma(a_1)$, где $\sigma = E_k|_A$ — сужение отображения E_k на множество A. Покажем, что в случае $L > 2$ отображение E_k на всем множестве A^2 представимо либо в виде

$$E_k|_{A^2} = \sigma,$$

либо в виде

$$E_k|_{A^2} = \sigma \circ \mu.$$

Рассмотрим такой случай: пусть найдутся такие $a_1, a_2 \in A$, $a_1 \neq a_2$, что

$$E_k(a_1a_2) = \sigma(a_1)\sigma(a_2).$$

Покажем, что тогда $E_k|_{A^2} = \sigma$. Для начала докажем, что в этом случае $E_k(a_1a) = \sigma(a_1)\sigma(a)$ для любого $a \in A$. Предположим, что это не так. Тогда найдется такое $a \in A$, $a \neq a_1$, $a \neq a_2$, что $E_k(a_1a) = \sigma(a)\sigma(a_1)$. Рассмотрим слово $a_1a_2a \in A^3$. Так как

$$\varepsilon(a_1a_2a) = \{a_1a_2, a_1a, a_2a\},$$

то

$$E_k(\varepsilon(a_1a_2a)) = \{\sigma(a_1)\sigma(a_2), \sigma(a)\sigma(a_1), E_k(a_2a)\}.$$

Поскольку $E_k(\varepsilon(a_1a_2a)) = \varepsilon(E_k(a_1a_2a))$ (лемма 7) и слово $E_k(a_1a_2a)$ однозначно определяется по множеству $\varepsilon(E_k(a_1a_2a))$ (лемма 8), то либо слово $E_k(a_2a)$ должно начинаться на букву $\sigma(a_1)$, либо на букву $\sigma(a)$. Так как

$$E_k(a_2a) \in \{\sigma(a_2)\sigma(a), \sigma(a)\sigma(a_2)\},$$

то $E_k(a_2a) = \sigma(a)\sigma(a_2)$ и поэтому $E_k(a_1a_2a) = \sigma(a)\sigma(a_1)\sigma(a_2)$. Теперь рассмотрим слово $a_1aa_2 \in A^3$. Так как

$$\varepsilon(a_1aa_2) = \{a_1a, a_1a_2, aa_2\}$$

и $E_k(aa_2) = \sigma(a_2)\sigma(a)$, то

$$E_k(\varepsilon(a_1aa_2)) = \{\sigma(a)\sigma(a_1), \sigma(a_1)\sigma(a_2), \sigma(a_2)\sigma(a)\}.$$

Но из полученного множества нельзя собрать слово, так как в данном множестве три слова начинаются на три различные буквы, а этого не может быть (лемма 8). Так как должно быть $E_k(\varepsilon(a_1aa_2)) = \varepsilon(E_k(a_1aa_2))$, то слова $E_k(a_1aa_2)$ не существует. Противоречие.

Таким же образом показывается, что $E_k(aa_2) = \sigma(a)\sigma(a_2)$ для любого $a \in A$. Пусть $ab \in A^2$. Тогда $E_k(a_1b) = \sigma(a_1)\sigma(b)$, а из данного равенства будет следовать равенство $E_k(ab) = \sigma(a)\sigma(b)$.

Совершенно аналогично доказывается, что если найдутся такие $a_1, a_2 \in A$, $a_1 \neq a_2$, что

$$E_k(a_1a_2) = \sigma(a_2)\sigma(a_1),$$

то $E_k|_{A^2} = \sigma \circ \mu$.

Таким образом, условие пункта 2 доказано для всех слов из множества $A \cup A^2$. Предположим, что условие пункта 2 верно для всех слов из множества $A \cup \ldots \cup A^t$, где $t < l$. Докажем утверждение для случая $t = l$. Пусть для определенности $E_k|_{A \cup \ldots \cup A^t} = \sigma$. Зафиксируем $x \in A^l$. Из леммы 7 следует, что

$$E_k(\varepsilon(x)) = \varepsilon(E_k(x)).$$

Исходя из предположения индукции и леммы 7, имеем:

$$E_k(\varepsilon(x)) = \sigma(\varepsilon(x)) = \varepsilon(\sigma(x)).$$

Из полученного равенства $\varepsilon(E_k(x)) = \varepsilon(\sigma(x))$ немедленно вытекает равенство $E_k(x) = \sigma(x)$ (лемма 8).

Если же $E_k|_{A^l} = \sigma \circ \mu$, то

$$\varepsilon(E_k(x)) = E_k(\varepsilon(x)) = (\sigma \circ \mu)(\varepsilon(x)) = \varepsilon((\sigma \circ \mu)(x)).$$

Поэтому $E_k(x) = (\sigma \circ \mu)(x)$. В силу произвольности элемента $x \in A^l$ получаем справедливость утверждения пункта 2. Теорема доказана.

Следствие 1. *Пусть* $X = Y = \bigcup_{l=1}^{\infty} A^l$. *Эндоморфный шифр* Σ_A *не распространяет искажений типа пропуска знаков тогда и только тогда, когда для любого* $k \in K$ *либо*

$E_k = \sigma$ на всем множестве X,

либо

$E_k = \sigma \circ \mu$ на всем множестве X,

где $\sigma = E_k|_A$ — сужение отображения E_k на множество A.

Шифры, не распространяющие искажений типа вставки знаков

Введем на множестве X бинарное отношение ε следующим образом. Пусть $x, y \in Y$. $x \varepsilon y \Leftrightarrow$ слово x получено из y путем добавления одной буквы.

Как и прежде, определим множество $\varepsilon(x)$ для некоторого $x \in X$ следующим образом:

$$\varepsilon(x) = \{y \in X \mid x \varepsilon y\}.$$

Определение 4. *Будем говорить, что шифр* Σ_A *не распространяет искажений типа вставки знаков, если для любых* $x, y \in Y$, *любого* $k \in K$ *и любого натурального* n *найдется такое число* $0 \le m \le n$, *что из условия* $x \varepsilon^n y$ *следует* $D_k(x) \varepsilon^m D_k(y)$.

Очевидно, что все леммы из предыдущего пункта будут справедливы и для шифров, не распространяющих искажений типа вставки знаков. Поэтому доказательство следующей теоремы аналогично доказательству теоремы 2.

Теорема 3 (Бабаш А.В., Глухов М.М., Шанкин Г.П.**).** *Пусть* $X = Y = \bigcup_{i=1}^{L} A^i$. *Эндоморфный шифр* Σ_A *не распространяет искажений типа вставки знаков тогда и только тогда, когда для любого* $k \in K$ *выполнены следующие условия:*

1. Если $L=2$, то для любого $x\in X$ либо

$$E_k(x)=\sigma(x),$$

либо

$$E_k(x)=\sigma(\mu(x)),$$

где $\sigma=E_k|_A$ — сужение отображения E_k на множество A;

2. Если $L>2$, то либо

$$E_k=\sigma \text{ на всем множестве } X,$$

либо

$$E_k=\sigma\circ\mu \text{ на всем множестве } X,$$

где $\sigma=E_k|_A$ — сужение отображения E_k на множество A.

Следствие 2. *Пусть* $X=Y=\bigcup_{l=1}^{\infty}A^l$. *Эндоморфный шифр* Σ_A *не распространяет искажений типа вставки знаков тогда и только тогда, когда для любого* $k\in K$ *либо*

$$E_k=\sigma \text{ на всем множестве } X,$$

либо

$$E_k=\sigma\circ\mu \text{ на всем множестве } X,$$

где $\sigma=E_k|_A$ — сужение отображения E_k на множество A.

Из теорем 1, 2, 3 получается такое

Следствие 3. *Пусть*

$$X=Y=\bigcup_{l=1}^{L}A^l,\ L>2, \quad \text{либо} \quad X=Y=\bigcup_{l=1}^{\infty}A^l.$$

Тогда если шифр Σ_A не распространяет искажений типа пропуска (вставки) знаков, то он также не распространяет искажений типа замены знаков.

Список литературы

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. – М.: Гелиос АРВ, 2005, 480 с.

2. Бабаш А.В., Глухов М.М., Шанкин Г.П. О преобразованиях множества слов в конечном алфавите, не размножающих искажений// Дискретная математика, 1997. Т. 9. No 3. С. 3–19.

3. Рацеев С.М. Некоторые обобщения теории Шеннона о совершенных шифрах // Вестн. ЮУрГУ. Сер. Матем. моделирование и программирование. 2015. Т. 8. No 1. С. 111–127.

References

1. Alferov A.P., Zubov A.Yu., Kuz'min A.S., Cheremushkin A.V. Foundations of Cryptography. Moscow, Gelios ARV, 2005. 480 p.

2. Babash A.V., Glukhov M.M., Shankin G.P. On transformations of a set of words in a finite alphabet that do not propagate distortions // Diskr. Mat., 1997. V. 9. No 3. Pp. 3–19.

3. Ratseev S.M. Some generalizations of Shannon's theory of perfect ciphers // Vestnik YuUrGU. Ser. Mat. Model. Progr., 2015. V. 8. No 1. P. 111–127.